NAVAL WAR COLLEGE
Newport, R.I.

Network Centric Warfare – Wiring Joint Forces for Battle: Are Operational Leaders Really Plugged In?

by

Thomas F. Keeley
Captain, U.S. Navy

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature: T. Keeley

16 May 2000

3 A

REPORT DOCUMENTATION PAGE

1. Report Security Classification: UNCLASSIFIED

2. Security Classification Authority: N/A

3. Declassification/Downgrading Schedule: N/A

4. Distribution/Availability of Report: DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.

5. Name of Performing Organization:
JOINT MILITARY OPERATIONS DEPARTMENT

6. Office Symbol: C

7. Address: NAVAL WAR COLLEGE
686 CUSHING ROAD
NEWPORT, RI 02841-1207

8. Title (Include Security Classification): Network Centric Warfare – Wiring Joint Forces for Battle: Are Operational Leaders Really Plugged In? (U)

9. Personal Authors:
CAPT Thomas F. Keeley, USN

10.Type of Report: FINAL

11. Date of Report: 16 May 00

12.Page Count: [redacted]24

12A Paper Advisor (if any): CAPT M.L. Felmy, USN (Initial guidance)

13.Supplementary Notation: A paper submitted to the Faculty of the NWC in partial satisfaction of the requirements of the JMO Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

14. Ten key words that relate to your paper:
Cultural Change, Education, Information Operations, Information Superiority, Information Systems, Leadership, Network Centric Warfare, Relevant Information, Shared Awareness, Technical Competency.

15.Abstract:

Network Centric Warfare, a concept for the information age, uses "Metcalfe's Law;" *the value of a network is directly proportional to the square of its nodes* as its basis for achieving Information Superiority. This concept, though, does not adequately address the "technical competency" of an essential node in military informational networks: leaders.

This paper puts forth a case that leaders are nodes in the network and they must understand both the network and the information for their actions to add real value.

16.Distribution / Availability of Abstract:	Unclassified X	Same As Rpt	DTIC Users

17.Abstract Security Classification: UNCLASSIFIED

18.Name of Responsible Individual: CHAIRMAN, JOINT MILITARY OPERATIONS DEPARTMENT

19.Telephone: 841-6461

20.Office Symbol: C

Security Classification of This Page Unclassified

Abstract of

Network Centric Warfare – Wiring Joint Forces for Battle:
Are Operational Leaders Really Plugged In?

Network Centric Warfare, a concept for the information age, uses "Metcalfe's Law;" *the value of a network is directly proportional to the square of its nodes* as its basis for achieving Information Superiority. This concept, though, does not adequately address the "technical competency" of an essential node in our informational networks: leaders.

This paper puts forth a case that leaders are nodes in the network and they must understand both the network and the information for their actions to add real value.

Table of Contents

Bibliography

Abramson, Gary. "Seen the light?" *CIO Enterprise Magazine,* 15 June 1999, 8.

Alberts, David S., John J. Garstka, and Frederick P. Stein. *Network Centric Warfare: Developing and Leveraging Information Superiority*. Washington, D.C.: National Defense University Press, 1999.

Allard, Kenneth. "Information Operations in Bosnia: A Preliminary Assessment." *Strategic Forum*, no. 91 (November 1996): 1-4.

Bernstein, Alvin H., Martin Libicki, and Fredrick W. Kagan. "High-tech: The future face of war? – A debate." *Commentary*, Jan 1998, 28-34.

Cheswick, Bill and Steven Branigan. "Bell Laboratories Internet Mapping Project." 29 June 1999 <http://www.cs.bell-labs.com/who/ches/map/> (21 April 2000).

Gentry, John A. "Knowledge-based warfare: Lessons form Bosnia." *The Officer* 75, no. 1 (Feb 1999): 137-142.

Hubbard, Zachary P. "Information Warfare in Kosovo," *Journal of Electronic Defense,* Nov 1999, 57-60.

Kouzes, James M. and Barry Z. Posner. *Credibility: how leaders gain and lose it, why people demand it.* San Francisco: Jossey-Bass Publishers, 1993.

Levien, Frederic H. "Kosovo: An IW Report Card," *Journal of Electronic Defense,* Aug 1999, 48-49.

Libicki, Martin C. *Illuminating Tomorrow's War*. Washington, DC: National Defense University Press, 1999.

National Academy of Sciences, "Volume 4: Human Resources, Chapter Two," *Technology for the United States Navy and Marine Corps, 1997.* <http://books.nap.edu/html/tech_21st/hr2.htm> (4 April 1999).

National Aeronautics and Space Administration. *Program / Project Management Development Process Support Materials Handbook*, September 1999 <http://appl.nasa.gov/pmdp/handbook/guide.htm> (18 April).

Negroponte, Nicholas. *Being Digital*. New York: Knopf, 1995.

Olsen, Florence. "Learn to Think Algorithmically," *The Chronicle of Higher Education*, 23 March 1999. <http://chronicle.com/free/2000/03/20003220lt.htm> (4 April 2000).

Pillsbury, Michael. *China Debates the Future Security Environment*. Washington, D.C.: National Defense University Press, 1999.

Schein, Edgar H. "The Three Cultures of Management: The Key to Organizational Learning," *Sloan Management Review*, Fall 1996. <http://mitsloan.mit.edu/smr/past/1996/smr3811.html> (6 April 2000).

Senge, Peter M. *The Fifth Discipline*. New York: Doubleday, 1990.

Shaw, Eric D., Jerrold M. Post, and Keven G. Ruby. *Final Report: Insider Threats to Critical Information Systems*, 31 August 1999. Political Psychology Associates, 98-G-7900.

Slater, Robert. *The New GE*. Homewood: Richard D. Irwin, 1993.

Stamps, David. "A conversation with doctor paradox," *Training*, May 1997, 42-48.

Sun Tzu. *The Art of War*. New York: Oxford University Press, 1963.

U.S. Commission on National Security/21st Century. "New World Coming: American Security in the 21st Century." Washington, D.C.: GPO, 15 September 1999.

U.S. Department of Defense. *Final Report on Information Assurance and Information Technology*. Washington, D.C.: GPO, 9 July 1999.

________. *Kosovo/Operation Allied Force After-Action Report*. Washington, D.C.: GPO, 31 January 2000.

U.S. Joint Chiefs of Staff. *Joint Vision 2010*. Washington, D.C.: GPO, 1995.

________. *Concept for Future Joint Operations*. Washington, D.C.: GPO, May 1997.

________. *Doctrine for Intelligence Support to Joint Operations*, (Joint Publication 2-0) Washington, D.C.: GPO, 5 May 1995.

________. *Information Assurance through Defense in Depth*. Washington, D.C.: GPO, February 2000.

________. *Information Operations - Strategy for Peace, the Decisive Edge in War*. Washington, D.C.: GPO, 1999.

________. *Joint Doctrine for Information Operations*. (Joint Publication 3-13) Washington, D.C.: GPO, 1997.

Vego, Milan. *On Operational Art*. Newport: U.S. Naval War College, 1999.

Zimm, Alan D. 'Human-Centric Warfare," *Proceedings* 125, no. 5 (May 1999): 155-158.

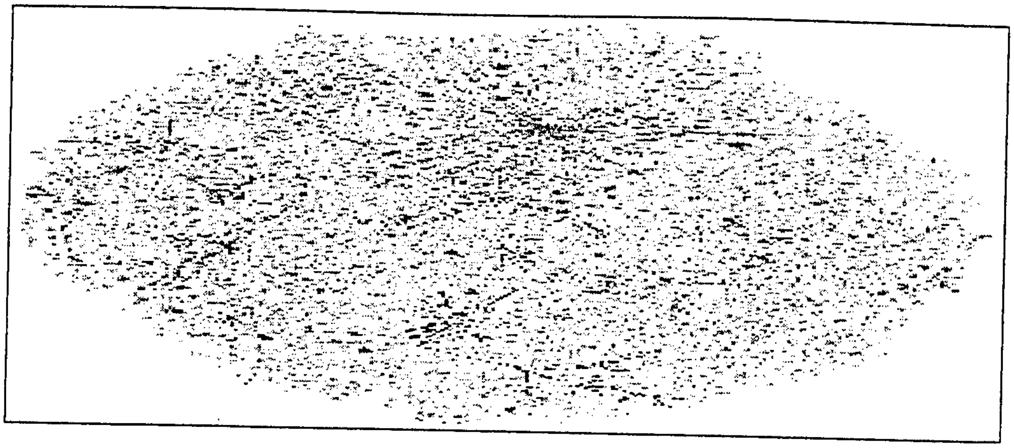
Chapter 1 - *Introduction*

Network Centric Warfare (NCW) is a new information age concept, which systematically wires joint forces together for battle. This idea theorizes our forces will utilize technological innovation to gain information superiority over any future adversary. NCW will create *shared battlespace awareness and knowledge* through a global interconnection of sophisticated networks.[1]

NCW ignites numerous discussions about its viability as a warfare concept ranging from the technological implications to, recently, the human interconnection. However, little has come forth on the technical competencies required, especially of leaders, to realize these prophesized gains.

The advantages of NCW are based upon "Metcalfe's Law"*; the value of a network is directly proportional to the square of its nodes.*[2] Therefore, NCW suggests the more nodal interactions a network has then the value of awareness and knowledge information increases exponentially throughout the network.[3]

Systems engineers can design and pictorially display elaborate networks depicting millions of nodes. The depiction seldom shows the most important node in any information network: the user. The individual user is left out. They do not appear as part of the intricate network structure since the connection or interaction is implied. The picture below, an interactively mapped depiction of the Internet as it appeared to engineers at Bell Laboratories in June of 1999, clearly illustrates this point.[4]



This figure shows a snapshot in time of the information flow process among the ever-growing lash up of servers throughout the world.[5] It is a simple visualization of *Metcalfe's Law* in action, growing exponentially each month, spreading information and knowledge.[6] It is the commercial *infostructure* that spawns a revolution in business affairs and helps spark NCW's concept of a self-synchronizing system of systems[7] -- a system striving to create shared awareness for its users, at the speed of light.

Operational commanders, as leaders in the information age, must gain an awareness of how this example of what NCW professes affects the operational factors of military operations.[8] How do the operational factors of space, time and forces apply to this new battlespace? Today's leaders somehow have to know this. For they too are connected as a node, some would say the critical node, in the very system NCW is attempting to replicate.[9] If a leader, connected as a node in the network, is not technically competent, is there value added? Do the nodes have to intelligently interact to satisfy Metcalfe's summation? Common sense would tell us yes, and statistical analysis verifies that position.

Intelligent interaction would imply a leader requires a skill, ability or competence to do so.[10] In today's information frenzied global environment, fueled by an ever-changing *electronic bazaar* of gadgetry and *techno-jargon*, leaders must have technical competency just to survive, let alone interact.[11] Yet, NCW merely mentions a requirement of learning *new attitudes and skills* in the future.[12] Well, what do leaders whom are designing, procuring, managing or using information on systems or networks right now need? The answer according to a nationwide survey of more than 1500 mangers provides three recurring responses: 1st - integrity, 2nd -competence, and 3rd - leadership.[13] A follow-up study of over 800 executives yields the exact same results. The more technical the nature of the business the more technical competency becomes a factor in leadership requirements.[14]

Technical competency is a functional expertise that applies to a person's job content.[15] Job content for an operational commander can apply to a myriad of new information age requirements. Commanders must now synthesize new warfare methodologies and acronyms, dealing with the synchronization of bytes, into old warfare areas dealing with the destruction of atoms.[16] A solid understanding of technology and information superiority would seem appropriate for leaders to employ these new approaches in military operations.[17]

Chapter 2 - *Technology and Information Superiority*

The emerging evidence for Network Centric Warfare as the intellectual basis for Joint Vision 2010 is compelling. General Hugh Shelton, CJCS, June 22, 1999.

We really should look at where the concept of NCW originated. *Joint Vision 2010* (JV 2010) is its genesis, providing a vision of how our military would fight in the 21st Century.[18] This vision depends upon the proper use of two enablers, innovative technologies and information superiority, allowing operational commanders to succeed in any situation, at any time.[19] NCW appears to simply take JV 2010's enablers and apply new age business practices of retailers and investment firms to fashion a realization of information superiority.[20]

Information superiority (IS) is the *capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same.*[21] Denying access to information is very a difficult goal and a major problem that the very companies NCW claims to emulate, struggle with daily. A recent Department of Defense (DoD) report on Information Assurance takes a close look at several recent military exercises (*Solar Sunrise, Eligible Receiver, and Evident Surprise*) and determines that the prospects for achieving IS within DoD are *bleak.*[22]

During these exercises, numerous successful attacks are staged against various DoD networks. Analysis of the actual techniques and entry points used to gain access into these various systems points to one common node.

Exploitation of weakness in the technical competencies or security procedures of individuals, not equipment, allow access to the systems.[23] The study goes on to address one more point:

> *The most important segment of the Departments workforce that requires IT (Information Technology) awareness training is the senior leadership: flag and general officer and SES. These are individuals who shape the priorities and make the decisions that impact the IT initiatives within their mission areas. Not knowing the capabilities, limitations or regulatory requirements regarding IT initiatives puts the department at risk for additional problems. The department must insure that adequate skills, knowledge, and awareness of IT are woven throughout the organizations and not just at the IT functional levels.*[24]

The Naval Studies Board, during their recent study of information technologies, reaches the exact same conclusion when addressing the requirement for technical competency throughout the Navy:

> *It is tempting to assume that flag and general officers, as the most senior military executives, have reached a level of mastery that transcends any need for further education and training. Such an assumption is, in a word, wrong, and given the level of authority and responsibility held by general and flag officers can easily lead to disaster in the rapidly evolving environments of naval operations.*[25]

NCW is a tremendous IT initiative. To achieve success in its implementation, our forces and especially our leaders require a simple shared understanding of just how IT helps us gain IS, as the studies suggest. The knowledge, skills and awareness, which leaders need to obtain the goal of IS, are not found among NCW's literature. They appear in a Joint Staff publication called the *Concept for Future Joint Operations* (CFJO). CFJO requires the integration of three separate components to achieve IS: *Information Systems, Relevant Information, and Information Operations.* [26] Raising awareness and technical competency in these three components is perhaps, a methodology for plugging our leaders into NCW's concept.[27]

Chapter 3 - *Information Systems*

> *Information Systems are the architectures and functions for collecting,* processing, analyzing, archiving, and disseminating information.[28]

Communications and computer technology is what comes to mind when information systems are talked about. Rapid expansion of technologies throughout the world is causing us to reassess the operational factor of space.[29] This new space, commonly referred to as cyberspace, is where digital age visionaries insist we must now operate.[30] It is filled with an ever-changing interconnection of highly technical systems ranging from satellites to handheld communications devices. It contains systems of people connected and communicating through technology. Leaders need to understand that people are information systems too.

People are looking to leaders for information. They seek an understandable vision for the way in which a leader sees technology evolving. This may require leaders to learn to communicate in an entirely new fashion. For they now must have more than a passive understanding of these systems to help their organizations effectively function in the information age. [31]

The recent conflict in Kosovo (*Operation Allied Force*) provides insight into the utilization of information systems to achieve the goals of JV 2010 and NCW. This operation presents warfighters with an unparalleled employment of sophisticated information systems.[32] Despite this impressive array of systems, significant shortfalls still occur in the areas of information management, systems integration, network security, and utilization of newly fielded systems all reportedly due to a lack of understanding of the technologies involved.[33]

Sun Tzu professes *those who do not know the conditions of mountains and forests, hazardous defiles, marshes and swamps, cannot conduct the march of an army.*[34] He is saying leaders must have knowledge of the space in which they intend to operate to move through it successfully. Space has continually evolved from Sun Tzu's time with the introduction of new technologies. The areas of operations today involve outer space and the informational realm of cyberspace.

The movement through cyberspace creates justifiable concerns surrounding the competent operation of our information systems. These concerns are driven by the proliferation of knowledge information, outsourcing of information systems, and the dizzying technical nature of the systems we rely on.[35] No country is as widely wired with a growing dependence on information systems for basic economic, social and defense functions as ours.[36] This fact has not escaped the scrutiny of adversaries like China. The Chinese believe we will not achieve IS due to: *too much inter-service rivalry, insufficient funding, the technology is too complex, and our information networks are too vulnerable.*[37]

These four simple insights could become relevant bits of information as we continue to plug new systems into our forces. American industry has already found that an organization can be *IT rich, but informationally inept.*[38]

Chapter 4 - *Relevant Information*

Relevant information is the full range of necessary information about friendly forces, the enemy, the operations area, and anything else that affects operational decision making.[39]

Relevant information is intelligence that applies to what you are trying to do at any given time. In battle, you are trying to out maneuver your adversary.[40] To do this, Sun Tzu recommends, *"know the enemy and know yourself."*[41] Knowing the enemy entails developing an understanding of everything about his *goals, objectives, strategy, intentions, capabilities, methods of operation, vulnerabilities, and sense of value and loss*[42]in respect to time.

Knowing yourself can necessitate recognizing what to know and when to know it. Our sources of relevant information are caught in a never-ending quest, by the gods of technological breakthroughs, to better see the battlespace.[43] We are focusing toward working for technology rather than the reverse.[44] A good example comes from operations in Bosnia:

> *Such priorities meant, for example, that the decision to deploy a state-of-the-art intelligence system known as Trojan Spirit with the U.S. brigades was delayed until shortly before those units left for Bosnia. Although such impressive technologies provide a compelling way to enlarge the information highway to the lower echelons, such well-intended "fixes" must be balanced against the realities of Bosnia's 24-hours-a-day operations. A tactical intelligence officer said, "We just don't have time over here for any more visits by the Good Idea Fairy." The larger point: advances in information technology are of military value only to the extent that they are accompanied by coherent doctrine, organizations, equipment, and people--to say nothing of the time needed to make them function as a team.*[45]

The Bosnian experience is ripe with examples of poor intelligence competencies such as: disregard for lessons learned, lack of training, inept processing and analytical techniques, disbelief of non-military or open source information, and finally jointness issues.[46] Quoting a lesson learned best summarizes the reason behind these deficiencies: *poor minimal use of available information and lack of concern about knowledge-related deficiencies suggest that the key obstacle to all information, or knowledge-based military operations, is the brains of leaders.*[47]

Chapter 5 - *Information Operations*

Information operations (IO) involve actions taken to affect adversary information and information systems while defending one's own information and information systems.[48]

Information Operations (IO) is an integrating strategy for the application of information, procedures or weapons against atoms, bytes and minds.[49] It is the synchronization of all elements of our national power through extensive use of relevant information and information systems to create a desired effect in the mind of an adversary. That effect should prevent conflict. If conflict arises, then the capabilities and related activities of IO become Information Warfare (IW). The goal of IO though, is to prevent IW, and that requires comprehensive prior planning and coordination throughout our government before the conflict begins.

The problem surrounding IO's utilization stems from a widespread lack of understanding of how to use this new application of force. The prevailing train of thought is that IO is simply computer network attack. Joint Publication 3-13 (Information Operations) was published in October of 1998 and has still not gained acceptance throughout the services. A separate publication nicknamed the "toilet book," specifically published by the Joint Staff, to enhance the IO knowledge of senior leadership has not produced the desired effect.[50] Ardent du Picq states in Battle Studies, *the instruments of battle are valuable only if one knows how to use them.*[51]

Recent operations in Kosovo show leaders do not understand how to synchronize IO's components into force. DoD's latest report to Congress cites lack of advanced planning, knowledge deficiencies, and no clear guidance from leadership as hindrances to the execution of IO there.[52] Some additional competency considerations concerning specific areas of IO/IW are:

A. Operational Security. → Numerous security vulnerabilities relating to operations, communications, computers, information, and information assurance are directly related to either a lack of technical competency or misuse of manual security procedures.[53]

B. Operational Deception. → Technology exchange has created a situation of "is it real or is it Memorex?" Computer processing capabilities coupled with software for morphing and digital manipulation of images will dramatically alter this age-old expertise.[54]

C. Psychological Operations. → Reserve components in our military carry out the majority of this mission. Their use of television broadcasts and leaflets during Kosovo is ineffective due to a lack of planning for terrain and weather conditions.[55]

D. Destruction. → Adversaries have transitioned to camouflage, decoys, working among the civilians, and underground networks to challenge our capabilities here. It has become a game of *hide and seek warfare.*[56]

E. Electronic Warfare. → The technological exchange of information is spawning developments in the areas of electromagnetic pulse weapons and laser technology capable of temporarily disrupting intelligence sensors.[57]

F. Computer Network Attack. → The recent *Melissa* and *Love Bug* viruses best demonstrate the transparency of information flow throughout the world. Thousands of computer attack techniques are available, free of charge, on the Internet. These programs can turn anyone who can "point and click" into a computer hacker in minutes. Legal considerations and complications are extensive and require sage counsel in this area.

G. Civil Affairs. → Reserve components, for the most part, handle this perception management tool. Kosovo operations prove its utility to the warfighter.[58] The increasing probability of missions other than war requires further integration of these capabilities into all our forces.

H. Public Affairs. → This area has moved from print to television through technology. This capability relies upon the creation of believability and trust through appearance: a science called telegenics. Absolute creditability is the key to success. Actions in Kosovo show most of our military leaders are ill skilled in this science.[59]

Attainment of the knowledge and skills required for the IS advantage is a cause for concern given unknown appropriations and retention problems currently facing the military. The more daunting problem though, may actually arise from the changes required in the intangibles of attitude and culture.

Chapter 6 – Attitudes and Culture

When a new technological challenge faces an organization, leaders with technical competence are strongly preferred.[60] They do not have to be technology geeks. They must simply take time to learn and really know all aspects of current operations before they make an irreversible and costly decision. Leaders must know their capabilities. If they lack any, they must constantly learn with the organization to realize that it is the workers, not the leaders, who decide if the leaders are competent.[61]

Attitudes help set the stage for initial learning and change.[62] Some of the common attitudes surrounding the elements of IS are:

- Technology → "I do not need to learn about computers. I have done fine without it so far."
- Intelligence → "I'll know what I need to know when I see it."
- Information Operations → "It is just computers."

Education and training to correct these perceptions are underway throughout DoD. Why then, do organizations fail to learn? Experts contend it is not due to people's resistance to change, their nature, or poor leadership. It is due to communication. Lack of communication between cultures in an organization leads to failure when the cultures collide.[63]

NCW visionaries look at cultures of companies such as Wal-Mart in fashioning their new concept.[64] Wal-Mart has an existing shared awareness due to strong-stable leadership, clear vision, consistent workers, and continuous efforts at customer and employee satisfaction before they ever plug into the information age though.[65]

The sculptors of NCW instead, should look at the cultural transformation that occurred at General Electric (GE). GE, a global company, has similarities to the military in terms of bureaucratic structure. It has a long corporate culture resistant to change: the GE way is the only way.[66] Yet, in 1981, Jack Welch, a technically competent leader, assumes the reigns and immediately embarks on a course to transform GE's social architecture and consciousness through education, communication, and pursuit of quantifiable quality.[67]

His now world-renowned *Six Sigma Black Belts,* a process based upon communication and quality, reverses GE's bureaucratic culture using these simple premises: [68]

- *Customers decide quality*
- *Involve everyone in the game*
- *Those closest to the work know it best*
- *Educate, educate, educate from within*
- *Be number one or number two in whatever you do*

Welch's credible involvement of all GE employees in his vision allowed them to see both the value and need for change. He successfully applied the philosophy of management specialist Peter Drucker to deal with competition facing his organization with a *shift from the command and control organization, the organization of departments and divisions, to the information-based...organization of knowledge specialists."*[69] GE still maintained a hierarchical structure of authority but, *"authority, like information, is not lost once distributed. You can share it, yet still have it."*[70]

Welch succeeds because he nurtures competencies in all aspects of his organization. He learns that, *"people cannot contribute to the aims and aspirations of an organization if they do not know what to do, and they cannot help if they do not know how to do it. They need skills and abilities to perform.*[71] He transforms GE into a *learning company*; a company running on shared awareness and the synchronization of focused efforts.

Chapter 7 – *Conclusions*

A. Counter arguments

Leaders can get by with generalized skills. They have done this in the military for years because good leaders can inspire their way to success. They are heroes rising to the occasion in times of crisis.[72]

B. Rebuttal

Operation Restore Hope in Somalia presents our leaders an adversary who understands IS. Their adversary, Mohammed Aideed, combines the elements of information systems (a video camera), relevant information (our adversity to dead soldiers) and information operations (Destruction, Psychological Operations and Public Affairs) to defeat a technologically superior force. Aideed competently synchronizes information with the operational factors of time, space, and force to achieve victory. He shows the value of a technically competent leader in a simple network. Unfortunately, our leaders do not.

C. Recommendations and Closing

As both technology and information continue to expand around us, perhaps a simpler process for the integration of NCW's concept is called for. Recommend the following approach to deal with the issue of technical competency requirements for leaders and our entire force:

- Create a vibrant learning environment which demands technical competence in the three components of IS throughout our entire force structure.
- Stress technical competence, algorithmic thinking, communication, project management and team building skills in this environment.
- Treat **everyone as an operator** with value to add to the network.
- Shift to Network Centered Forces using information systems, relevant information and information operations to achieve Information Superiority vice NCW.
- Reorganize staff structures around the three elements of IS.

- Plug fellow services, interagency and allies into networks as customers who you must satisfy at all times.
- Stop buying systems for technology's sake. Learn to use and fully integrate the systems we already have. Then plug in off the shelf technology that is compatible with our system, mission, and vision.
- Manage the system as a whole, not parts and pieces.
- Remember low tech hurts too!

Information age concepts will continue to surround leaders. They must look at what their missions are. They must listen to their people. They must learn to apply present "systems" to their vision. They must competently plug into what is going on all around them if we are ever going to achieve IS. Think about it. ***Look. Listen. Learn. Lead.***

Notes

[1] David S. Alberts, John J. Garstka, and Frederick P. Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority* (Washington, D.C.: National Defense University Press, 1999), 86.
[2] Ibid., 29.
[3] Ibid., 31.
[4] Bill Cheswick and Steve Branigan, *Bell Laboratories Internet Mapping Project*, 29 June 1999. <http://www.cs.bell-labs.com/who/ches/map/> (21 April 2000).
[5] Ibid.
[6] Alberts, 31.
[7] Ibid., 166.
[8] Milan Vego, *On Operational Art* (Newport: U.S. Naval War College, 1999), 53-54.
[9] Alan D. Zimm, "Human-Centric Warfare," *Proceedings* 125, no. 5 (May 1999): 155-158.
[10] Florence Olsen, "Learn to Think Algorithmically," *The Chronicle of Higher Education*, 23 March 1999. <http://chronicle.com/free/2000/03/20003220lt.htm> (4 April 2000).
[11] Martin C. Libicki, *Illuminating Tomorrow's War*, (Washington, D.C.: National Defense University Press, 1999), 15-17.
[12] Alberts, 223.
[13] James M. Kouzes and Barry Z. Posner, *Creditability*, (San Francisco: Jossey-Bass, 1993), 12.
[14] Ibid.

[15] National Aeronautical and Aerospace Administration, Program/Project Management Development Process Support Materials Handbook, September 1999. <http://appl.nasa.gov/pmdp/handbook/guide.htm> (18 April 2000).
[16] Nicholas Negroponte, *Being Digital,* (New York: Knopf, 1995), 14.
[17] Joint Chiefs of Staff, *Concept for Future Joint Operations*, (Washington, D.C.: GPO, May 1997), 19.
[18] Joint Chiefs of Staff, *Joint Vision 2010,* (Washington, D.C.: GPO, 1995), 1.
[19] Ibid., 27.
[20] Alberts, 33.
[21] Joint Chiefs of Staff, *Joint Vision 2010*, 16.
[22] Department of Defense, *Final Report on Information Assurance and Information Technology,* (Washington, D.C.: GPO, 9 July 1999), 23.
[23] Ibid., 24.
[24] Ibid., 25.
[25] National Academy of Sciences, "Volume 4: Human Resources, Chapter Two," *Technology for the United States Navy and Marine Corps*, 1997. <http://books.nap.edu/html/tech_21st/hr2.htm> (4 April 1999).
[26] Joint Chiefs of Staff, *Concept for Future Joint Operations*, 39.
[27] National Academy of Sciences.
[28] Joint Chiefs of Staff, *Concept for Future Joint Operations*, 39.
[29] Vego, 54.
[30] Libicki, 71.
[31] Peter Senge, *The Fifth Dimension* (New York: Doubleday, 1990), 12-13.
[32] Department of Defense, *Kosovo / Operation Allied Force After-Action Report,* (Washington, D.C.: GPO, 31 January 2000), 46.
[33] Ibid., 46-51.
[34] Sun Tzu, *The Art of War* (New York: Oxford University Press, 1963), 104.
[35] Eric D. Shaw, Jerrold M. Post, and Keven G. Ruby, Final Report: Insider Threats to Critical Information Systems, 98-G-7900, (Bethesda, MD: Political Psychology Associates, 31 August 1999), 13-16.
[36] Commission on National Security/21st Century, *New World Coming* (Washington, D.C.: GPO, 15 September 1999), 120.
[37] Michael Pillsbury, *China Debates the Future Security Environment*, (Washington, D.C.: National Defense University Press, 1999), 66.
[38] Gary Abramson "Seen the light?" *CIO Enterprise Magazine*, 15 June 1999, 8.
[39] Joint Chiefs of Staff, *Concept for Future Joint Operations*, 40.
[40] Joint Chiefs of Staff, *Doctrine for Intelligence Support to Joint Operations*, (Joint Publication 2-0), (Washington, D.C.: GPO, 5 May 1995.), II-1.
[41] Sun Tzu, 84.
[42] Joint Chiefs of Staff, (Joint Publication 2-0), II-1.
[43] Alvin H. Bernstein, Martin Libicki, and Fredrick W. Kagan, "High-tech: The future face of war? – A debate," *Commentary*, Jan 1998, 34.
[44] Ibid.
[45] Kenneth Allard, "Information Operations in Bosnia: A Preliminary Assessment, " *Strategic Forum,* November 1996, 4.
[46] Jon A. Gentry, "Knowledge-based warfare: Lessons from Bosnia," *The Officer* 75, no.1 (Feb 1999): 137-142.
[47] Ibid., 142.
[48] Joint Chiefs of Staff, *Joint Doctrine for Information Operations*, (Joint Publication 3-13), (Washington, D.C.: GPO, 9 October 1998), I-3.
[49] Ibid.

[50] Joint Chiefs of Staff, *Information Operations. Strategy for Peace, The Decisive Edge in War*, (Washington, D.C.: GPO, 1998), I-3.

[51] Joint Chiefs of Staff, *Information Assurance through Defense in Depth*, (Washington, D.C.: GPO, February 2000), 12.

[52] Department of Defense, *Kosovo/Operation Allied Force After-Action Report*, 98-99.

[53] Ibid., 75-77.

[54] Negroponte, 128-129.

[55] Frederic H Levien, "Kosovo: An IW Report Card," *Journal of Electronic Defense*, Aug 1999, 48-49.

[56] Libicki, 15.

[57] Libicki, 18-19.

[58] Zachary P. Hubbard, "Information Warfare in Kosovo," *Journal of Electronic Defense*, Nov 1999, 57-58.

[59] Hubbard, 58.

[60] Kouzes and Posner, 17.

[61] Ibid., 69.

[62] Ibid., 34.

[63] Edgar H. Schein, "The Three Cultures of Management: The Key to Organizational Learning," *Sloan Management Review*, Fall 1996.
<http://mitsloan.mit.edu/smr/past/1996/smr3811.html> (6 April 2000).

[64] Alberts. 33.

[65] David Stamps, "A conversation with doctor paradox," *Training*, May 1997, 42-48.

[66] Ibid.

[67] Robert Slater, *The New GE* (Homewood: Richard D. Irwin, 1993), 120-140.

[68] Ibid.

[69] Ibid., 169.

[70] Stamps, 47.

[71] Kouzes and Posner, 17.

[72] Senge, 340.